IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	Criminal No. 1:23-CR-108
v.	Count 1: 18 U.S.C. § 371 Conspiracy to Commit Offenses Against the United States
MAKSIM SILNIKAU a/k/a Maksym Silnikov a/k/a "targa" a/k/a "klm" a/k/a "lansky" a/k/a "xxx" a/k/a "J.P.MORGAN," *Defendant.*	Counts 2-3: 18 U.S.C. § 1343 Wire Fraud Count 4: 18 U.S.C. § 1349 Conspiracy to Commit Wire Fraud Count 5: 18 U.S.C. § 1029(b)(2) Conspiracy to Commit Access Device Fraud Counts 6-7: 18 U.S.C. § 1028A(a)(1) Aggravated Identity Theft Forfeiture Notice UNDER SEAL

INDICTMENT

June 2023 Term – at Alexandria, Virginia

COUNT ONE

(Conspiracy to Commit Offenses Against the
United States – 18 U.S.C. § 371)

THE GRAND JURY CHARGES THAT:

1. MAKSIM SILNIKAU, a/k/a Maksym Silnikov a/k/a "targa" a/k/a "klm" a/k/a "lansky" a/k/a "xxx" a/k/a "J.P.MORGAN," is the creator and administrator of the Ransom Cartel ransomware strain, which was created in 2021. SILNIKAU, a Belarusian national, has been a member of Russian-speaking cybercrime forums since at least 2005 and was a member of the

notorious and elite cybercrime website Direct Connection from 2011 until 2016, when the site was shuttered after the arrest of its administrator.

General Allegations

2. Unless otherwise noted, at all times relevant to this Indictment:

a. SILNIKAU used numerous monikers and names on various cybercrime websites during his involvement in the Russian-speaking cybercriminal underground. A moniker is a chosen username or nickname. Using a moniker across platforms allows career cybercriminals like SILNIKAU to enter into illegal transactions anonymously while generating goodwill and credibility among fellow cybercriminals around their use of their moniker.

b. "Ransomware" is a type of malicious software that enables a cybercriminal to encrypt a victim's computer and/or remove data from the victim's computer so that the cybercriminal can demand ransom payments in exchange for decrypting the computer and/or not disseminating the data. Cybercriminals use cryptographic algorithms to encrypt the victim's computer files so the only way to decrypt the data is with the cryptographic key controlled by the cybercriminal. Cybercriminals engaged in ransomware often steal and sell the encrypted data to others, despite promising victims that the data has been deleted after the ransom is paid.

c. "Ransomware-as-a-service" is a cybercrime practice of individuals specializing in various skills that are used to promote and carry on ransomware attacks. With such specializations, one individual need not be responsible for all of the various cybercrime skills, but instead can pay others for assistance in particular specializations. Some of these specializations include ransomware operators, hackers, initial access brokers, botnet operators, crypters, and others.

d. An "initial access broker" is a specific type of cybercrime-as-a-service provider who obtains and sells access to victim computer networks. Hackers who exploit that

access can use it to carry out ransomware attacks, other types of damage, fraud, or theft. Initial access brokers use a variety of means, including botnets, to obtain initial access to the victim networks.

e. A "crypter" is another type of ransomware-as-a-service provider who specializes in recoding malware so it will function normally but won't be recognized and detected by antivirus programs. This process is sometimes referred to as "packing" the malware so it can avoid detection from the antivirus program.

f. A "loader" is a piece of malware or a cybercriminal that specializes in installing or "loading" malware such as ransomware or botnet malware on to victim computers.

g. A "cybercrime forum" is a website used by people involved in cybercrime to discuss and commit criminal activities. Generally, forum members register anonymously by creating a moniker, and will typically provide an email address during the registration process to receive correspondence related to forum activity, or as a means of account recovery if they forget their password or are locked out of their accounts. Cybercrime forums are typically where those who specialize in particular services that support ransomware-as-a-service meet to engage each other's services.

h. Forum A was a cybercrime forum.

i. Victim 1 was a company located in New York.

j. Victim 2 was a company located in California.

k. All amounts of currency, dates, and times are approximate.

The Conspiracy and its Objects

3. From May 2021 until the present, in the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM SILNIKAU, a/k/a Maksym Silnikov a/k/a "targa" a/k/a "klm" a/k/a "lansky" a/k/a "xxx" a/k/a "J.P.MORGAN,"

did knowingly and intentionally combine, conspire, confederate, and agree with others known and unknown to the Grand Jury to commit the following crimes:

a. to intentionally access a computer without authorization, and thereby obtain information from a protected computer, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the laws of the United States, contrary to Title 18, United States Code, Section 1030(a)(2)(C), (c)(2)(B)(i), (ii);

b. to knowingly cause the transmission of a program, information, code, and command, and as a result of such conduct, intentionally cause damage without authorization, contrary to Title 18, United States Code, Section 1030(a)(5)(A);

c. to intentionally access a protected computer without authorization, and as a result of such conduct, cause damage and loss, contrary to Title 18, United States Code, Section 1030(a)(5)(C); and

d. to transmit, with intent to extort from a person any money and thing of value, in interstate or foreign commerce, a communication containing (1) threat to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access and (2) a demand and request for money and a thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, contrary to Title 18, United States Code, Section 1030(a)(7)(B), (C).

4. The purpose of the conspiracy was to unlawfully obtain money and property by obtaining unauthorized access to victims' computers, installing ransomware on those computers, and then demanding that victims pay a ransom.

Manner and Means of the Conspiracy

5. It was part of the conspiracy that SILNIKAU coordinated the development of the Ransom Cartel ransomware.

6. It was further part of the conspiracy to advertise on cybercrime forums, including Forum A.

7. It was further part of the conspiracy that SILNIKAU negotiated with initial access brokers to obtain a supply of potential ransomware victims.

8. It was further part of the conspiracy that SILNIKAU distributed cybercrime tools, including lockers, loaders, and crypters to co-conspirators.

9. It was further part of the conspiracy that SILNIKAU established and maintained a panel, which was a hidden website where SILNIKAU and his co-conspirators could monitor and control ransomware attacks, communicate with co-conspirators, manage payouts to co-conspirators, and communicate with victims.

10. It was further part of the conspiracy that SILNIKAU and his co-conspirators negotiated agreements about payment from successful acts of extortion.

11. It was further part of the conspiracy that SILNIKAU and his co-conspirators installed ransomware on victims' computers, exfiltrated their data, and then encrypted or "lock" the computers.

12. It was further part of the conspiracy that after a victim's computers were locked, SILNIKAU and his co-conspirators contacted the victim and demanded payment in cryptocurrency.

13. It was further part of the conspiracy that ransom paid to SILNIKAU and his co-conspirators in cryptocurrency was transferred repeatedly, including through services called "mixers," to prevent law enforcement from identifying the owner of the cryptocurrency.

14. It was further part of the conspiracy that SILNIKAU established a hierarchy for co-conspirators who used his ransomware, including a ratings system that rewarded productive co-conspirators.

Overt Acts in Furtherance of the Conspiracy

15. In furtherance of the conspiracy, and to accomplish the objects thereof, SILNIKAU and his co-conspirators committed within the Eastern District of Virginia and elsewhere the following overt acts in furtherance of the conspiracy, among others.

16. Starting in May 2021, SILNIKAU developed a ransomware-as-a-service operation. At that time, SILNIKAU began recruiting participants from cybercrime forums.

17. On May 4, 2021, the conspiracy posted a public advertisement to Forum A in Russian seeking access to compromised corporate computer networks located in the United States and elsewhere. The advertisement is translated from Russian as follows:

> Will buy access to corporate networks.
> Will buy access to corporate networks in the following countries: US, CA, UK, AU, ZN, EU, and other countries except for CIS [Commonwealth of Independent States].
>
> Access rights: Domain Admin, Local Admin, User
> Revenue: from $10 million
> Prices from $100 and up.
> Not interested in previously sold accesses.
> Will consider working with you on commission (%)
> I conduct all deals only through the guarantor service of this forum. Guarantor service will be paid for by me.
>
> In order to save your time and mine, PM me the following information:
>
> GEO (geolocation):
> Revenue:
> Access rights:
> Contact information (jabber or TOX):

18. On various occasions during 2021 and 2022, SILNIKAU distributed information to Ransom Cartel participants about compromised computers, including stolen credentials, that he was considering as targets for Ransom Cartel ransomware.

19. On or about July 15, 2021, SILNIKAU referred a potential co-conspirator to an administrative panel that could be used to control ransomware locker software.

20. On various occasions during 2021 to 2023, SILNIKAU negotiated payment terms with individuals whom he was recruiting for his ransomware operation. For instance, on April 25, 2023, SILNIKAU negotiated with a potential co-conspirator about payment terms on which to provide access to computers for locking.

21. On or about November 16, 2021, SILNIKAU executed a ransomware attack on Victim 1.

22. In late 2021, SILNIKAU changed the name of his ransomware operation to "Ransom Cartel" and sought to publicize it on cybersecurity news sites.

23. On or about March 5, 2022, Ransom Cartel ransomware was deployed against Victim 2. The hackers removed confidential data without authorization and demanded a monetary payment to refrain from releasing the victim's data.

(All in violation of Title 18, United States Code, Section 371.)

COUNTS TWO and THREE

(Wire Fraud – 18 U.S.C. § 1343)

24. Paragraphs 1, 2 and 16 through 23 of this Indictment are re-alleged and incorporated as if fully set forth here.

25. On or about the following dates, within the Eastern District of Virginia and elsewhere,

MAKSIM SILNIKAU a/k/a Maksym Silnikov a/k/a "targa" a/k/a "klm" a/k/a "lansky" a/k/a "xxx" a/k/a "J.P.MORGAN,"

having devised and intending to devise a scheme and artifice to defraud, and for obtaining money by means of materially false and fraudulent pretenses, representations, and promises, as set forth below, did transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds.

The Scheme and Artifice

26. It was part of the scheme and artifice that SILNIKAU developed ransomware.

27. It was further a part of the scheme and artifice that SILNIKAU would distribute cybercrime tools, including lockers, loaders, and crypters, to potential co-conspirators.

28. It was further part of the scheme and artifice that SILNIKAU and his accomplices would negotiate agreements about payment to result from successful extortions involving his ransomware infrastructure.

29. It was further a part of the scheme and artifice that SILNIKAU would establish and maintain a "panel," which was a hidden website where SILNIKAU and his accomplices could monitor and control ransomware attacks, communicate with co-conspirators, manage payouts to accomplices, and communicate with victims.

30. It was further a part of the scheme and artifice for SILNIKAU would obtain stolen credentials from initial access brokers for the purpose of accessing victims' computer systems without authorization.

31. It was further a part of the scheme and artifice for SILNIKAU and his accomplices would use the stolen credentials to falsely represent to victims' computer systems that they were persons who were authorized to access the systems.

32. It was further a part of the scheme and artifice that SILNIKAU and his accomplices would escalate their privileges on the victims' computer systems, thereby obtaining administrative access.

33. It was further part of the scheme and artifice that SILNIKAU and his co-conspirators would install ransomware on victims' computers, exfiltrate their data, and then encrypt or "lock" the computers.

34. It was further part of the scheme and artifice that after a victim's computers were locked, SILNIKAU and his co-conspirators would contact the victim and demand payment in cryptocurrency.

//

//

//

//

//

//

//

//

Execution of the Scheme and Artifice

35. On or about the dates specified below as to each count, in the Eastern District of Virginia and elsewhere, SILNIKAU did, for the purpose of executing the aforesaid scheme and artifice, transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, as described further below with respect to each count:

Count	Approximate Date	Wire Communication
2	7/15/2021	Message at 4:09pm referring potential co-conspirator to administrative panel for controlling ransomware locker software.
3	4/25/2023	Message at 9:18pm negotiating with potential co-conspirator about terms on which to provide access to computers for locking.

(All in violation of Title 18, United States Code, Section 1343.)

COUNT FOUR

(Conspiracy to Commit Wire Fraud – 18 U.S.C. § 1349)

36. Paragraphs 1, 2, 5 through 23, and 26 through 34 of this Indictment are re-alleged and incorporated as if fully set forth here.

37. From May 2021 until the present, in the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM SILNIKAU a/k/a Maksym Silnikov a/k/a "targa" a/k/a "klm" a/k/a "lansky" a/k/a "xxx" a/k/a "J.P.MORGAN,"

did knowingly and intentionally combine, conspire, confederate, and agree with others known and unknown to the Grand Jury, to commit wire fraud; that is, that having devised and intending to devise any scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce certain writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, contrary to Title 18, United States Code, Section 1343.

(All in violation of Title 18, United States Code, Section 1349.)

COUNT FIVE

(Conspiracy to Commit Access Device Fraud – 18 U.S.C. § 1029(b)(2))

THE GRAND JURY FURTHER CHARGES THAT:

38. Paragraphs 1, 2, 5 through 23, and 26 through 34 of this Indictment are re-alleged and incorporated as if fully set forth here.

39. From May 2021 until the present, within the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM SILNIKAU a/k/a Maksym Silnikov a/k/a "targa" a/k/a "klm" a/k/a "lansky" a/k/a "xxx" a/k/a "J.P.MORGAN,"

did knowingly and intentionally combine, conspire, confederate, and agree with others known and unknown to the Grand Jury: (a) to knowingly and with intent to defraud traffic in one or more unauthorized access devices during a one-year period, and by such conduct obtain a thing of value aggregating $1,000 or more during that period, in violation of Title 18, United States Code, Section 1029(a)(2); and (b) to knowingly and with intent to defraud possess fifteen or more devices which are unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3); and at least one of the parties engaged in any conduct in furtherance of such offense, affecting interstate and foreign commerce.

(All in violation of Title 18, United States Code, Section 1029(b)(2).)

COUNTS SIX and SEVEN

(Aggravated Identity Theft – 18 U.S.C. § 1028A(a)(1))

THE GRAND JURY FURTHER CHARGES THAT:

40. On the dates set forth below, within the Eastern District of Virginia and elsewhere, the defendant,

MAKSIM SILNIKAU a/k/a Maksym Silnikov a/k/a "targa" a/k/a "klm" a/k/a "lansky" a/k/a "xxx" a/k/a "J.P.MORGAN,"

did, during and in relation to a felony violation contained in chapter 63 of Title 18, United States Code, that is, a violation of Title 18, United States Code, Section 1349, as charged in Count Four of this indictment, knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, each count further described below:

Count	Date	Means of Identification
6	7/15/2021	Username and password of K.W.
7	7/15/2021	Username and password of S.W.

(All in violation of Title 18, United States Code, Section 1028A(a)(1).)

NOTICE OF FORFEITURE

Defendant MAKSIM SILNIKAU is hereby notified, pursuant to Federal Rule of Criminal Procedure 32.2(a), that upon conviction of the violations set forth in COUNTS ONE through FOUR of this Indictment, he shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461: any property, real or personal, which constitutes or is derived from proceeds traceable to such violations.

Defendant MAKSIM SILNIKAU is hereby notified, pursuant to Federal Rule of Criminal Procedure 32.2(a), that upon conviction of the violation set forth in COUNT FIVE of this Indictment, he shall forfeit to the United States, pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1029(c)(1)(C): (A) any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of the violation; and (B) any personal property used or intended to be used to commit the violation.

Pursuant to 21 U.S.C. § 853(p), MAKSIM SILNIKAU shall forfeit substitute property, if, by any act or omission of MAKSIM SILNIKAU, the property referenced above cannot be located upon the exercise of due diligence;

has been transferred, sold to, or deposited with a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.

(All in accordance with Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B), 1029(c)(1)(C); Title 21 United States Code, Section 853(p); Title 28 United States Code, Section 2461; and Fed. R. Crim. P. 32.2.)

A TRUE BILL:

Pursuant to the E-Government Act,
The original of this page has been filed
under seal in the Clerk's Office

Foreperson of the Grand Jury

JESSICA D. ABER
UNITED STATES ATTORNEY

Jonathan S. Keim
Zoe Bedell
Assistant United States Attorneys